Acumen.io

Acumen.io Security White Paper

At Acumen.io, the security of your data is our top priority. This paper provides an overview of Acumen's policies around data security and management.

Certifications

Acumen is ISO-certified, GDPR-compliant, and SOC 2 Type-2 pending.

Data security

How we collect and store data

Acumen uses publicly-available APIs to connect to data sources including source control, task management, and collaboration tools. Further documentation on the APIs we use can be found here:

- **Github**
- **Jira**
- **Slack**

Acumen stores only metadata related to projects and pull requests. We do not retain any source code.

Data hosting

Acumen data is hosted in the US region within the Google Cloud. Google Cloud's security infrastructure security design review – and policies towards encryption at rest and in transit and application layer transport – are documented **here**.

Data protection

Acumen encrypts data both in motion and at rest.

- **In transit:** in order to encrypt in-transit traffic, we use Transport Layer Security (TLS). Data being sent from a client, whether web-based or a mobile application, is sent over a secure HTTPS connection secured by a 4096-bit SSL certificate.
- **At rest:** Once any information has been sent from the client to our infrastructure, the data (personal information, messages, attachments) is securely stored in GCP using strong encryption standards. The data stored on the volumes, the disk I/O and the snapshots created from the volumes are all encrypted. The storage itself uses AES-256 encryption keys which are entirely managed and protected by the GCP KMS management infrastructure.

Network security

Acumen ensures the highest-level of network security through a multi-level approach:

- Firewalls and web security
- Intrusion detection system
- Contant vulnerability scanning for code, images and live servers
- Strict access controls for personnel
- Encrypted server-to-server communication via VPN
- Hardware security module based keys for encrypting sensitive data such as tokens and keys

Consumer Privacy Protection

Acumen captures and stores a limited range of end-user PII (name and email address) in order to:

- Unify data across services (e.g., using the same email address for both Github and Jira)
- Facilitate useful in-application displays and insights (e.g., show that user Foo worked on project Bar)

User data is encrypted as described above. Acumen provides full support for GDPR-related requests, including the right to be forgotten.